UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,291	08/16/2001	Marinus Frans Kaashoek	12221-005001	3137

26161 7590 10/18/2006

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,291	KAASHOEK ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 August 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-9,11-19,21,22 and 24-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-9,11-19,21,22 and 24-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendments

1. Applicants arguments with respect to presently pending claims 1, 3-9, 11-19, 21-22, and 24-27 filed on 08/04/2006 have been fully considered but are not persuasive.

2. The examiner's objection to the drawing, on the last action, was necessary and the objection still maintained because applicant is required to submit clearly numbered drawings not hand written to clearly read and understand the drawings.

3. The rejection to claims 1,3-9, 11-19, 21-22, and 24-27 under the judicially created doctrine of obviousness-type double patenting, as being unpatentable over claims 1-36 of co-pending application No. 09/931,561 is appropriate because the difference in the scope, wherein the "control center" in the instant claims and "central controller element" of the method claim 1 in the co-pending application, is minor and patentably indistinct and are directed to the same inventive concept. The subject matter of the narrower claim is fully disclosed in and covered by the broader claim of the reference.

Response to Arguments

4. Applicant's argument regarding applied reference, Greenwald 2003/0149919 A1, wherein "the fault engines are not the recited monitors and thus Greenwald does not teach a communication device that receives data from a plurality of monitors as claimed", as recited in claims 1, 9, 18, and 21 (remark page 1par. 2, and page 10 lines 17-19), are not persuasive. Greenwald's fault diagnosis engine receives data, collected from the network, from fault detectors 130 and fault handlers 150 based on agents (see, par. 0065-0070, and par. 0032).

5. Argument regarding applied reference, Greenwald, wherein "fault handlers and the fault diagnosis engine are not collecting statistical informational network traffic nor analyzing that information the control center", as recited in claims 1, 9, 18, and 21 (remark page 10 par. 3), is not persuasive because Greenwald discloses receiving and analyzing statistical information and/or fault data form detecting agents in a plurality networks (see, par. 0032-**0039**, **fig. 6B-C** and 0065-0070).

6. Argument regarding applied reference, Greenwald, wherein "a communication device, coupled to a physically separate network from the network that the data center is coupled, to receive data from a plurality of monitors dispersed through the network that the data center is coupled to, with the monitors sending data collected from the network that the data center is coupled to over the physically separate network from the network that the plurality of monitors collect data from", as recited in claims 1, 9, 18, and 21 (remark page 10 lines 16-25). The examiner disagrees. Greenwald teaches a fault handler engine, which is not in network 22, 24, 26, and 28, receiving fault/DOS data from plurality of agents in a plurality of networks for managing DOS (0039, fig. 6B-C, and 0068).

7. Argument regarding applied reference, Greenwald not teaching limitation, wherein "a process... to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic and an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data", as recited in claims 1, 9, 18, and 21 (remark page 11 lines 16-19). The examiner disagrees.

Greenwald teaches a system for detecting/identifying, diagnosing or managing faults in communication networks by determining network traffic statistics and identifying malicious traffic. Greenwald defines fault as a denial of service attacks/DOS, packet filtering, network blasters (i.e. entities emitting excessive amounts of traffic), obstacles (e.g., when one entity prevents another entity from achieving maximum throughput), state or misplaced static routing information, incorrect network policies, and etc. Greenwald clearly discloses packet filtering, monitoring gateway preventing traffic from being transmitted from first to second device upon detection (see, 0032, 0035, 0104, and fig. 6B-C).

8. Applicant's argument regarding applied reference, Messmer, failure to discloses the feature wherein "a control center to coordinate thwarting attacks on a victim data center..." as recited in claims 1, 9, 18, and 21 (remark page 12 lines 10-11). The examiner disagrees. Counterpane data center is used for a managed security service to identify DOS attacks or other threats. The Counterpane data center receives network activities from monitors/Counterpane box to determine if a consumer system/victim data center is under DOS attack (see, lines 1-20).

9. Applicant's argument regarding applied reference, Messmer, fails to teach the feature of the control center including: a computer system ...comprising... an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center" as recited in claims 1, 9, 18, and 21 (remark page 12 lines 14-17). The examiner disagrees. Messmer discloses receiving attack information from monitors/counterpane box and analyzing the received information to determine and identify the DOS attack on the target

consumer/victim data center (see, lines 4-32). And Yavatkar et al. discloses analyzing traffic on a network by monitoring network traffic when a particular network attack is detected by gathering information about the traffic on the network through redundant network (see, fig. 2), by launching an agent and having the agent iteratively identify which of the links on the node on which agent operates accepts a type of traffic, and traversing the identified link to the node across the link by halting, closing the path, shutting down, and/or installing appropriate filter on the monitor gateway (see col. 13 lines 54-col. 14 lines 32).

10. Applicant's argument regarding the examiner's contentions that "...coordination thwarting attacks is taught in Messmer, because Messmer teaches that the data center monitors network traffic to determine if the customers network is under attack", does not meet the claim language and fails to address the teachings in Messmer that "Counterpane staffers advice corporations on how to combat threats but do not make changes to the corporation's equipment." (remark page 12 par. 4) Examiner disagrees. Messmer teaches a managed security service of counterpane data center that identifies DOS attack based on information captured by monitors and transmitted to counterpane data center through different network (see, lines 5-49).

11. Applicant's argument regarding the examiner's contentions that "...Messmer teaches a hardened redundant network because the data collected is sent in encrypted from to the central control center" being different from the limitation "a communication device, coupled to a physically separate network from the network that the data center is coupled." (Remak page 13 par. 1-2 and page 15 par. 1). The examiner disagrees. Messmer teaches a communication device

(i.e. probe/black box)(see lines 17-26) to receive data from a plurality of monitors (see lines 23-26), dispersed through the network (see lines 23-27), the monitors sending data collected from the network over a hardened redundant network (see lines 23-28), Messmer teaches a hardened redundant network because the data collected is sent in encrypted form to the central control center (see lines 23-28). Messmer teaches the redundant network being a physically separate network from the network that the plurality of monitors collect data from, because the plurality of monitors are on the customers network (12-26), the central control center has its own network, that is in California or Virginia, where the data from the monitors is collected and sent to the data center (see lines 26-28). Moreover the limitation of claim 5 is canceled and not claimed.

12. Applicant's argument regarding Yavatker reference failure to disclose "flittering to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center" (remarks page 13par. 4-page 14 par. 2), is not persuasive. Yavatkar et al. discloses analyzing traffic on a network by monitoring network traffic when a particular network attack is detected by gathering information about the traffic on the network through redundant network (see, fig. 2), by launching an agent and having the agent iteratively identify which of the links on the node on which agent operates accepts a type of traffic, and traversing the identified link to the node across the link by halting, closing the path, shutting down, and/or installing appropriate filter on the monitor gateway (see col. 13 lines 54-col. 14 lines 32).

13. Regarding applicant's argument concerning Yavatkar teaches away from any combination of a "sniffer" device arguing that it is a conventional method and is slow (remark

page 14 par. 4). Examiner disagrees. Yavatkar et al. discloses analyzing traffic on a network by monitoring network traffic when a particular network attack is detected by gathering information about the traffic on the network through redundant network (see, fig. 2).

14. Regarding applicant's argument concerning Messmer reference failure to disclose "sampled packets or statistical information about traffic flows, and the firewall and intrusion detection systems" (remarks page 14 par. 6). The examiner disagreesMessmer teaches a central control center (i.e. Counterpane data center)(see lines 26-28) to coordinate thwarting attacks(see lines 1-20), coordinating thwarting attacks is taught in Messmer, because Messmer teaches that the data center monitors network traffic to determine if the customers network is under attack. Messmer teaches a victim data center, because Messmer teaches that outsourcing intrusion detection, one company that does this is Counterpane, Counterpane monitors customers network (see lines 12-15), the customers network is the victim data center. Messmer teaches a communication device (i.e. probe/black box)(see lines 17-26) to receive data from a plurality of monitors (see lines 23-26), dispersed through the network (see lines 23-27).

Double Patenting

15. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re*

Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

16. Claims 1, 3-9, 11-19, 21-22, 24-27 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-36 of copending Application No. 09/931,561. Although the conflicting claims are not identical, they are not patentably distinct from each other because the application '561 teaches all the claims limitation except the differences that are underlined in the following table as an example:

Instant application 09/931291	**Copending application 09/931,561**
1. A system, comprising: • a **control center** to coordinate thwarting attacks on a victim data center that is coupled to a network, the control center including: • a communication device to receive data from a **plurality of monitors**, dispersed through the network, with the monitors sending data collected from the network, with the monitors sending data collected from the network over a redundant network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from;	1. A method of thwarting denial of service attacks on a victim data center coupled to a network, the method comprising: • monitoring network traffic through **monitors** disposed at a plurality of points in the network; • communicating data from the monitors to a **central controller**, over a redundant network, that is a different network from the network being monitored; • analyzing the data comprising network traffic statistics to identify network traffic that is pert of a denial of service attack; and • filtering the network traffic based on results of <u>analyzing the network traffic to discard network traffic that is identified</u>

• a computer system, the computer system comprising: • a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic; and • analyzes and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center.	as part of the denial of service attack. 5. The method of claim 3 wherein monitoring network traffic through the gateway occurs at network entry points of victim data centers.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

17. The only difference between these two applications is that the copending application '561 has a broader claim limitation as underlined above and the instant application has narrower claim limitations. Wherein said identifying malicious traffic applicant describes the identifying malicious traffic and/or denial-of-service (DOS) being identical in the process (see, page 17 last paragraph) and the action performed upon identifying the DOS/malicious traffic being discarding network traffic and eliminating the malicious traffic are interpreted explicitly the same. And further applicant's protection of victim's data center is claimed on dependent claim 5 as shown above.

18. Claims 1, 3-9, 11-19, 21-22, 24-27 of the instant application are envisioned by copending Application No. '561 claims 1-36 in that claims 1-36 of the copending application contain all the limitations of claims 1, 3-9, 11-19, 21-22, 24-27 of the instant application. Claims 1, 3-9, 11-19,

21-22, 24-27 of the instant application therefore are not patently distinct from the copending application claims and as such are unpatentable for obvious-type double patenting.

Claim Rejections - 35 USC § 102

19. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

20. Claims 1, 9, 18, and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Greenwald et al. US PG PUBs 2003/0149919 A1.

Regarding claims 1, 9, 18, and 21 Greenwald et al. teaches a system, comprising:

a control center (**fault diagnosis engine**) to coordinate thwarting attacks (par. 0032; ***fault including Denial of Service Attacks***) on a victim data center that is coupled to a network (par. 0034 and fig. 2A; ***target***), the control center including:

a communication device (par. 0072; ***receiver fault diagnosis engine***), coupled to a physically separate network from the network that the data center is coupled (0068, 0039 and fig. 6, 6B-C; ***agents/detectors that reside externally from fault diagnosis engine, on a network 22...***), to receive data from a plurality of monitors (***plurality of fault engines*** *on fig. 3 element 150*), dispersed through the network that the data center is coupled to, with the monitors

sending data collected from the network, with the monitors sending data collected from the network that the data center is coupled to over the, physically separate network from the network that the plurality of monitors collect data from (par. 0032, 0025 and fig. 6; ***in a physically different network***);

a computer system, the computer system comprising:

a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic (par. 0032 and 0035; ***determination of faults/DOS by fault engines and fault diagnosis engine***); and

analyzes and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center (par. 0032, 0104 and fig. 6B-C; ***packet filtering, monitor gateway preventing traffic from being transmitted from first to second device upon detection***). And dependent claims are rejected based on dependency and/or other rejection in this Office Action.

Claim Rejections - 35 USC § 103

21. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

22. Claims 1, 3, 5-6, 9, 12-13, 18-19, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Messmer in view of Yavatkar et al. USPN 6,735,702 B1.

As per claims 1, 9, 18, 21, Messmer teaches a central control center (i.e. Counterpane data center)(see lines 26-28) to coordinate thwarting attacks(see lines 1-20), coordinating thwarting attacks is taught in Messmer, because Messmer teaches that the data center monitors network traffic to determine if the customers network is under attack. Messmer teaches a victim data center, because Messmer teaches that outsourcing intrusion detection, one company that does this is Counterpane, Counterpane monitors customers network (see lines 12-15), the customers network is the victim data center. Messmer teaches a communication device (i.e. probe/black box)(see lines 17-26) to receive data from a plurality of monitors (see lines 23-26), dispersed through the network (see lines 23-27), the monitors sending data collected from the network over a hardened redundant network (see lines 23-28), Messmer teaches a hardened redundant network because the data collected is sent in encrypted form to the central control center (see lines 23-28). Messmer teaches the redundant network being a physically separate network from the network that the plurality of monitors collect data from, because the plurality of monitors are on the customers network (12-26), the central control center has its own network, that is in California or Virginia, where the data from the monitors is collected and sent to the data center (see lines 26-28). Messmer teaches a computer system that includes a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic (see lines 28-32).

Messmer is silent on, filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center. However, Yavatkar et al. discloses

analyzing traffic on a network by monitoring network traffic when a particular network attack is detected by gathering information about the traffic on the network through redundant network (see, fig. 2), by launching an agent and having the agent iteratively identify which of the links on the node on which agent operates accepts a type of traffic, and traversing the identified link to the node across the link by halting, closing the path, shutting down, and/or installing appropriate filter on the monitor gateway (see col. 13 lines 54-col. 14 lines 32). It would have been obvious to one of ordinary skill in the art at the time of the invention to include Yavatkar et al.'s filtering process and eliminate the malicious traffic from entering the victim data center within the system of Messmer because it would block the attack targeted on the victim's computer. One would have been motivated to do so because it would further secure the victim's system from malicious attack that is sent over the hardened network.

As per claim 3, Messmer further teaches wherein the data analyzed by the control center is collected statistical information about network flows (see lines 29-30).

As per claims 4 and 11, Messmer further teaches wherein the control center aggregates in a computer system traffic information and coordinates measures to local and block the source of an attack (lines 1-20)

As per claim 5, Messmer further teaches wherein the physically separate is a telephone network (The examiner takes an official notice on the physically separate is a telephone network. Because it would have been obvious to one ordinary skill in the art at the time of the invention was made to apply the system of physically device of Messmer within a telephone

network because it would disclose the method in a telephone network to identify and filter attacks in a telephone network).

As per claim 6, Messmer further teaches wherein the monitors include gateways that are disposed at the victim data center and data collectors that are disposed in the network (see lines 12-25), the analysis process executed on the control center analyzes data from gateways and data collectors dispersed throughout the network (see lines 26-30).

As per claims 12, 19, Messmer further teaches receiving and analyzing are performed by a control center the computer system that is coupled to the data collectors via the hardened, redundant network (see lines 12-28).

As per claim 13, Messmer further teaches wherein plurality of monitoring devices (see lines 13-26); are data collectors dispersed throughout the network and at least one gateway device that is disposed adjacent the victim site to protect the victim (see lines 6-26), and wherein analyzing includes analyzing in the computer system data from the at least one gateway and the data collectors dispersed throughout the network (see lines 26-30).

Same Motivation applies above (see claim 1). Claim 18, is rejected under the same basis as claim 1. Further, Claim 18, is rejected for Malan disclosing determining a filtering process to eliminate the malicious traffic from entering the victim center; and aggregate traffic information and coordinating measures to locate and block sources of an attack (see col. 4, lines 60-65, col. 5, lines 43-53, col. 7, lines 1-6).

As per claim 21, limitations have already been addressed (see claims 1 and 18).

23. Claims 7-8, 14-16, 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Messmer in view of Yavatkar et al. USPN 6,735,702 B1 and further in view of Hill et al.

As per claims 7, 14, 24 Messmer does not disclose classifying attack. However, Hill et al. does disclose classifying attacks (see col. 5, lines 66-67, col. 6, lines 1-18). It would have been obvious to one of ordinary skill in the art at the time of the invention to include Hill et al. classifying attacks within the combination system of Messmer and Yavatkar et al., because classifying attacks displays attack information in a usable and quickly interpretable form to a network manager while minimizing the loading on the computer (see col. 2, lines 45-50 of Hill et al.). Therefore, by classifying attacks provides a network manager with knowledge of the severity and overall nature of the attack (see col. 2, lines 53-60 of Hill et al.).

As per claims 8, 15, 25 same motivations as above. Hill et al. further discloses wherein the classes of attack are denoted as low-grade with spoofing, low-grade without spoofing and high-grade whether spoofing or non-spoofing (see fig. 3, sheet 3, fig. 7, sheet 6).

As per claim 16, Messmer further teaches sending requests to gateways to send data pertaining to an attack to the control center (see lines 14-27).

Conclusion

24. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.
10/13/06

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/15/06